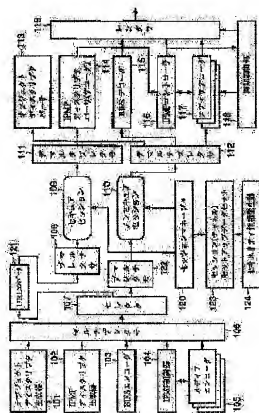


3

Priority number(s): JP20000273559 20000908

PROBLEM TO BE SOLVED: To realize multimedia transmission, while maintaining the safety of information which requires security. **SOLUTION:** Multimedia data, which is constituted of a plurality of objects and to which copyright protection information is added, is transmitted from a transmission side. A session-managing means for dividing multimedia data which are a stream outputted from the transmission side into copyright protection data and copyright non-protected data and managing a non-protected data transmission, a copyright-protected data, and a secure session transmitting copyright protection data are installed between the transmission side and a reception side.



<http://v3.espacenet.com/publicationDetails/biblio?DB=EPODOC&adjacent=true&l...> 2010/01/28

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-84516
(P2002-84516A)

(43) 公開日 平成14年3月22日 (2002.3.22)

| | | | |
|---------------------------|-------|---------------|-------------------|
| (51) Int.Cl. ⁷ | 識別記号 | F I | デフォルト (参考) |
| H 0 4 N 7/167 | | G 0 6 F 12/14 | 3 2 0 A 5 B 0 1 7 |
| G 0 6 F 12/14 | 3 2 0 | H 0 4 N 7/167 | Z 5 C 0 5 9 |
| H 0 4 N 7/08 | | 7/08 | Z 5 C 0 6 3 |
| 7/081 | | 7/13 | Z 5 C 0 6 4 |
| 7/24 | | | |

審査請求 未請求 請求項の数15 O L (全 16 頁)

(21) 出願番号 特願2000-273559 (P2000-273559)

(22) 出願日 平成12年9月8日 (2000.9.8)

(71) 出願人 000001007

キヤノン株式会社
東京都大田区下丸子3丁目30番2号

(72) 発明者 安藤 勉

東京都大田区下丸子3丁目30番2号キヤノ
ン株式会社内

(74) 代理人 100076428

弁理士 大塚 康徳 (外2名)

Fターム (参考) 5B017 AA03 BA10 CA16

5C059 KK43 MA00 MB00 RB02 RC00

SS20 UA01 UA04 UA38

5C063 AB03 DA07 DA13 DA20

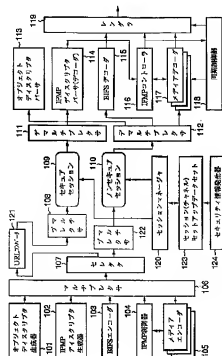
5C064 CA14 CB01 CC01 CC04

(54) 【発明の名称】 マルチメディアデータ送信装置及び方法、マルチメディアデータ受信装置及び方法、マルチメディアデータ伝送システム並びに記憶媒体

(57) 【要約】

【課題】 セキュリティを要する情報の安全性を保ちつつ、マルチメディア伝送を行うことが可能になる。

【解決手段】 送信側からは複数のオブジェクトで構成され、著作権保護情報が付加されたマルチメディアデータを送信する。そして、送信側と受信側との間には、送信側から出力されたストリームであるマルチメディアデータを、著作権保護データと非著作権保護データとに分割し、非著作権保護データの伝送を行う非セキュアセッション及び著作権保護データの伝送を行うセキュアセッションを管理するセッション管理手段を設ける。



【特許請求の範囲】

【請求項 1】 複数のオブジェクトで構成されるマルチメディアデータを送信するマルチメディアデータ送信装置であって、

知的財産保護管理データが付加されたマルチメディアデータをビットストリームとして入力する入力手段と、入力したビットストリームのマルチメディアデータを、知的財産保護管理データとそれ以外のメディアデータとに分割する分割手段と、

前記知的財産保護管理データと前記メディアデータとのリンク情報を更新するリンク情報更新手段と、前記メディアデータデータの伝送を行う非セキュアセッション及び前記知的財産保護管理データの伝送を行うセキュアセッションを管理するセッション管理手段とを備えることを特徴とするマルチメディアデータ送信装置。

【請求項 2】 前記セッション管理手段は、前記知的財産保護管理データに対してセキュアであることを示す識別子を含んだセッション情報データセットを設けることを特徴とする請求項第 1 項に記載のマルチメディアデータ送信装置。

【請求項 3】 前記マルチメディアデータは、MPEG-4 フォーマットのデータであることを特徴とする請求項第 1 項又は第 2 項に記載のマルチメディアデータ送信装置。

【請求項 4】 マルチメディアデータを受信するマルチメディアデータ受信装置であって、

非セキュアセッションによりメディアデータを受信する第 1 の受信手段と、

セキュアセッションにより前記メディアデータに対する知的財産を保護管理する知的財産保護管理データを受信する第 2 の受信手段と、

前記非セキュアセッション及び前記セキュアセッションを管理するセッション管理手段と前記セッション管理手段により、前記非セキュアセッションを介して受信したメディアデータを、各メディアストリームに分割し、デコードする第 1 の処理手段と、

前記セッション管理手段により、前記セキュアセッションを介して受信した知的財産保護管理データをデコードする第 2 の処理手段と

前記第 1、第 2 の処理手段によりデコードされたデータに基づいて再生する再生手段とを備えることを特徴とするマルチメディアデータ受信装置。

【請求項 5】 複数のオブジェクトで構成されるマルチメディアデータを送信するマルチメディアデータ送信方法であって、

知的財産保護管理データが付加されたマルチメディアデータをビットストリームとして入力する入力工程と、入力したビットストリームのマルチメディアデータを、知的財産保護管理データとそれ以外のメディア知的財産データとに分割する分割工程と、

前記知的財産保護管理データと前記メディアデータとのリンク情報を更新するリンク情報更新工程と、

前記メディアデータデータの伝送を行う非セキュアセッション及び前記知的財産保護管理データの伝送を行うセキュアセッションを管理するセッション管理工程とを備えることを特徴とするマルチメディアデータ送信方法。

【請求項 6】 請求項第 5 項に記載の各工程に対応するプログラムコードを格納すること特徴とする記憶媒体。

【請求項 7】 マルチメディアデータを受信するマルチメディアデータ受信方法であって、

非セキュアセッションによりメディアデータを受信する第 1 の受信工程と、

セキュアセッションにより前記メディアデータに対する知的財産を保護管理する知的財産保護管理データを受信する第 2 の受信工程と、

前記非セキュアセッション及び前記セキュアセッションを管理するセッション管理工程と前記セッション管理工程により、前記非セキュアセッションを介して受信したメディアデータを、各メディアストリームに分割し、デコードする第 1 の処理工程と、

前記セッション管理工程により、前記セキュアセッションを介して受信した知的財産保護管理データをデコードする第 2 の処理工程と、

前記第 1、第 2 の処理工程によりデコードされたデータに基づいて再生する再生工程とを備えることを特徴とするマルチメディアデータ受信方法。

【請求項 8】 請求項第 7 項に記載の各工程に対応するプログラムコードを格納すること特徴とする記憶媒体。

【請求項 9】 複数のオブジェクトで構成されるマルチメディアデータを送信するマルチメディアデータ送信装置であって、

メディアデータと、前記メディアデータの知的財産保護管理のための知的財産保護管理データとを入力する入力手段と、

前記メディアデータの伝送を行う非セキュアセッション及び前記知的財産保護管理データの伝送を行うセキュアセッションを管理するセッション管理手段とを備えることを特徴とするマルチメディアデータ送信装置。

【請求項 10】 前記セッション管理手段は、前記知的財産権保護データに対してセキュアであることを示す識別子を含んだセッション情報データセットを設けることを特徴とする請求項第 9 項に記載のマルチメディアデータ送信装置。

【請求項 11】 前記マルチメディアデータは、MPEG-4 フォーマットのデータであることを特徴とする請求項第 9 項又は第 10 項に記載のマルチメディアデータ送信装置。

【請求項 12】 複数のオブジェクトで構成されるマルチメディアデータを送信するマルチメディアデータ送信

方法であって、
マルチメディアデータと、前記マルチメディアデータの
知的財産保護管理のための知的財産保護管理データとを
入力する入力工程と、

前記マルチメディアデータの伝送を行う非セキュアセッ
ション及び前記知的財産保護管理データの伝送を行うセ
キュアセッションを管理するセッション管理工程とを備
えることを特徴とするマルチメディアデータ送信方法。

【請求項13】 請求項第12項に記載の各工程に対応
するプログラムコードを格納すること特徴とする記憶媒
体。

【請求項14】 複数のオブジェクトで構成されるマル
チメディアデータの伝送システムであって、
知的財産保護管理データが付加されたマルチメディアデ
ータをビットストリームとして入力する入力手段と、
入力したビットストリームのマルチメディアデータを、
知的財産保護管理データとそれ以外のメディアデータと
に分割する分割手段と、

前記知的財産保護管理データと前記メディアデータとの
リンク情報を更新するリンク情報更新手段と、
前記メディアデータの伝送を行う非セキュアセッション
及び前記知的財産保護管理データの伝送を行うセキュア
セッションを管理するセッション管理手段と、
前記非セキュアセッションを介して伝送されたメディア
データを、各メディアストリームに分割し、デコードする
第1の処理手段と、

前記セキュアセッションを介して受信した知的財産保護
管理データをデコードする第2の処理手段と、
前記第1、第2の処理手段によりデコードされたデータ
に基づいて再生する再生手段とを備えることを特徴とす
るマルチメディアデータ伝送システム。

【請求項15】 複数のオブジェクトで構成されるマル
チメディアデータの伝送システムであって、
メディアデータと、前記メディアデータの知的財産の保
護管理のための知的財産保護管理データとを入力する入
力手段と、

前記メディアデータの伝送を行う非セキュアセッション
及び前記知的財産保護管理データの伝送を行うセキュア
セッションを管理するセッション管理手段と、前記非セ
キュアセッションを介して伝送されたメディアデータ
を、各メディアストリームに分割し、デコードする第1
の処理手段と、

前記セキュアセッションを介して受信した知的財産保護
管理データをデコードする第2の処理手段と、
前記第1、第2の処理手段によりデコードされたデータ
に基づいて再生する再生手段とを備えることを特徴とす
るマルチメディアデータ伝送システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は知的財産（例えば、

著作権）保護管理データを含むマルチメディアデータの
伝送に関するものである。

【0002】

【従来の技術】現在、ISO/IEC 14496 (MPEG Phase 4)で
は、マルチメディアの符号化（圧縮フォーマット）の標
準化が進められている。本規格では、従来のビデオ・オ
ーディオデータの符号化のほかに、各メディアの空間・
時間的配置を定義することが可能であり、これをシーン
記述と呼んでいる。また、各々のメディアをオブジェク
トと呼称している。

【0003】図3に、シーンの一例を載せる。本例で
は、グラフィックオブジェクトとしてBOX（箱）301
およびCylinder（円柱）302、BOX301に貼付され
るイメージテクスチャ301a、Cylinder302に貼付
されるビデオテクスチャ302a、および同時に再生され
るオーディオ303が定義されている。

【0004】シーン記述自体の手法としては、VRML
(Virtual Reality Markup Language)を元に機能拡張
およびバイナリ化を行ったBIFS(Binary Format for S
cenesdescription)が採用されている。BIFSのバイナ
リ化方式については省略する。

【0005】また、このシーン記述とは別に、オブジェ
クトディスクリプタ（以降ODと呼ぶ）と呼ばれる、各
オブジェクトの属性を示すデータが付加される。属性と
は、メディアの属性（ビデオ、オーディオ、イメージな
ど）、知的財産権（例えば著作権、著作権、QoS (Qu
ality Of Service) 情報、コンテンツのレーティング情
報などである。これらの属性自体が、それぞれ1つの1
つのディスクリプタとして、ODの中に内包される。

【0006】図4にビットストリームの全体図の例を載
せる。

【0007】401は、初期オブジェクトディスクリプ
タであり、ビットストリーム全体のプロパティ（ビット
ストリームのプロファイルなど）を格納している。40
2はBIFSストリームであり、シーン情報を格納して
いる。

【0008】403及び406はODであり、以降のオ
ブジェクトの属性が記述される。本例では、2つのOD
(OD1、OD2)を持つ例を挙げている。OD1（4
03）、OD2（406）に続いて、各メディアストリ
ーム（これをエレメンタリストリームと呼んでいる）
ES1、ES2の属性を示すエレメンタリストリーム
ディスクリプタ（以降ESDと呼ぶ）が複数記述可能に
なっている。図4においては、OD1（403）の後に
ESD1（404）が記述され、OD2（406）の後に
ESD2（407）が記述されている。

【0009】また、エレメンタリストリームES1、
ES2については、実際にはパケットサイズされ、Sync L
ayer Packet（以降SLパケットと呼ぶ）として扱われ
るため、図4に示すようにSLパケットの構造を記述す

るためのSLConfigのディスクリプタ405、408がESD1(404)、ESD2(407)のそれぞれに対して付加される。

【0010】上述したOD及びESDのディスクリプタはそれぞれ、図4に示したビットストリームにおいて、各エレメンタリーストリームES1、ES2の前の先頭に設置する必要がある。ただし、OD及びESDはそれぞれ、ビットストリームの途中にアップデートコマンドを挿入することによって、追加、削除、及び変更が可能となっている。

【0011】また、規格では、各ODおよびESごとに、知的財産(例えば著作権)管理情報やアクセス制御情報を付加することが可能になっている。これをIPMP(Intellectual Property Management and Protection)情報と呼んでいる。IPMP情報自体も、IPMPディスクリプタと称されるディスクリプタにてその詳細が記述される。実際には、アクセス制御には暗号技術が使われるような例が多い。

【0012】ただし、IPMPの方式(ディスクリプタのシンタックス)は、特定されておらず、フリーシンタックスとなっている。ただし、RA(Registration Authority)に登録されたIPMPシステムタイプ番号だけを記述するようにになっている。

【0013】IPMPディスクリプタによって記述されたIPMP情報自体は、IDでリンクすることによって、IPMP用ES(IPMP_ES)を付加することが可能である。

【0014】図5は、この場合のビットストリーム全体の一例を示したものである。図5では、IPMP1(409)およびIPMP2(411)が、それぞれES1(410)、ES2(412)に対するIPMP_ESとなっている。また本例では、IPMP情報をアップデートする場合のコマンド513を1ヶ所含んだストリームの例を挙げている。

【0015】また、図6にIPMPディスクリプタの詳細例である。図中、601は、ディスクリプタタグ(TAG)であり、ディスクリプタの種類を示す。602は、レンジフィールド(LENGTH)であり、ディスクリプタ全体の長さ(バイト数)を示す。603は、ディスクリプタIDであり、ディスクリプタ自体のビットストリーム内でユニークな識別子を格納する。604は、IPMPSTYPEであり、前述したようにシステムタイプ番号を示す。605はオプションフィールド(Option)であり、IPMPに付随するデータを適宜挿入することができる。このフィールド605内のシンタックスが自由になっている。なお、付随データは、このフィールド605にURLとして外部に示すことも可能である。

【0016】上述したIPMPのディスクリプタについても、図5に示したビットストリームにおいて、各エレメンタリーストリームES1、ES2の前の先頭に設置

する必要がある。

【0017】図7に、これらのビットストリームを生成するためのシステムエンコーダの例を示す。

【0018】図中、701はオブジェクトディスクリプタ生成器であり、以上述べたようなディスクリプタをビットストリームのプロパティに応じて適宜生成する。702は、メディアエンコーダで、実際に、ビデオ、オーディオなどのデータをエンコードする。

【0019】704は、BIFSエンコーダであり、シーン情報をバイナリ化する。705は、アップデート制御部であり、必要に応じて、OD、ESD、IPMPディスクリプタなどのプロパティを更新するためのコマンドを挿入するが必ずしも、必須の機能ではない。706は、マルチプレクサであり、以上のディスクリプタや、メディアストリームを最終的に1つのSLパケットとしてマルチプレクスする部分である。

【0020】一方、図8にデコーダ(再生器)側の構成例を示す。図中、801は、マルチプレクサであり、各ディスクリプタ、ES等を分離する。803はディスクリプタバース(解析部)であり、タグ情報によってディスクリプタの種類を判別し、各ディスクリプタの内容を解釈し、適宜各部に設定する。804はBIFSデコーダであり、バイナリ化されたBIFSストリームをデコードし、シーン構造を再構築する。805はメディアデコーダであり、ビデオ、オーディオ、イメージなどのメディアデコーダを実際にデコードする部分である。

【0021】807はレンダラであり、シーン構造に従って各オブジェクトを、適宜表示・再生する機構である。806はIPMPコントローラである、IPMPディスクリプタおよびIPMP_ESの情報に従って、メディアの再生制御(再生制限、効果制御など)を行う。たとえば、暗号がかけられているような場合には、暗号を解読してからメディアデコーダにデータを転送する。

【0022】802は同期制御部であり、各メディア間の同期制御を行う。なお、図7のエンコーダ側から図8のデコーダ(再生器)側へのデータ転送方法については特記しないが、ネットワーク上の伝送の場合には、すべて1本のビットストリームとして同一セッションにて送受信されるのが一般的である。

【0023】一方、ISO/IEC 14496-6では、DMIFと呼ばれる端末とアプリケーションあるいは、端末間ネットワークの通信用のAPI(Application Programming Interface)を定義している。

【0024】図11にこのAPIの一例を示す。1101は、アプリケーションから新規チャネルを追加セットアップするインターフェースであり、1102は端末間のネットワーク間におけるチャネルセットアップインターフェースとなっている。1103は、ネットワーク上において、実際の通信プロトコルなどをセットアップするAPIである。

【0025】ここで、serviceSessionIdはチャネルを追加すべきセッションの識別子、qosDescriptorはチャネルのQOS(Quality Of Service)を示す記述子、directionは通信方向を示し、uDataInBuffer()は、追加情報を格納するバッファ、uDataInLenは前記バッファのデータ長を示す。また応答情報として、responseはチャネルセットアップの可否を示し、channelHandleはセットアップしたチャネルのハンドルを返し、uDataOutBuffer()は、追加情報を応答し、ddDataOutLenは前記バッファのデータ長を返す。このようにして、伝送プロトコルやセ

ットアップ手順に関わり無くチャネルをセットアップするためのAPIが定義されている。さらなる個々のパラメータについては、本件とは無関係であるので説明を省略する。

【0026】図15に、このAPIを用いた端末間のチャネルセットアップ手順を載せる。

【0027】アプリケーションは、DA_ChannelAdd()コマンドを用いて、チャネル追加要求を発行する。その後、DN_TransMuxSetup()コマンドによって、ネットワーク上のセットアップが行われる。DN_ChannelAdded()では、送受信端末間で実際にチャネルをセットアップする。

【0028】規格上は、最低限のパラメータ(セッションとチャネルの関係、伝送方向、QoS情報など)だけが定義されているが、実際には、さらにさまざまなパラメータを伝送することが必要になる。

【0029】また、図13に、このデータセットの一例を載せる。

【0030】DsmccMessageHeaderは、メッセージのヘッダである。NetworkSessionIDは、セッションの識別子を示す。ServiceIDは、さらに上位レイヤでのサービスのための識別子を示す。Countは、追加すべきチャネル数を示す。このチャネル数だけデータの繰り返しが行われ、各セッションのデータのメッセージが伝送される。

【0031】

【発明が解決しようとする課題】しかしながら、従来例では、それぞれ以下のような問題があった。

【0032】図6の例で、1PMPディスクリプタがブリーディングタックスのため、2つ以上の1PMPシステム間で互換性が取れないという問題があった。また、1PMPディスクリプタのシンタックスを明確に規格化してしまうと、セキュリティの方式が開示されるため、セキュリティレベルが下がってしまうという欠点があった。

【0033】また、図9に示すごとく、ネットワーク上を1PMPディスクリプタ(パケット)を伝送すると、ネットワーク上でデータを盗み見られて、セキュリティが保てなくなるといった欠点があった。901は、各ストリームを各工程(同期レイヤ:SL、可変長パケット生成部:FlexMux(図面ではFlexと記述されている)、およびネットワーク伝送用パケット生成部:TransMux

(図面ではTransと記述されている))に従ってマルチプレクスするマルチプレクサであり、最終的に1本のビットストリーム902が生成されることを示している。

尚、図9中に示されているAVOIはAudio Visual Objectを表す。Desc.は様々なディスクリプタを表す。

【0034】本発明はかかる問題点に鑑みながらなされたものであり、知的財産権(著作権)保護対象となるオブジェクトを含むマルチメディアデータの伝送において、その知的財産権保護対象となるオブジェクトに関する安全性を高めることを可能にするマルチメディアデータ送信装置及び方法、マルチメディアデータ受信装置及び方法、マルチメディアデータ伝送システム並びに記憶媒体を提供しようとするものである。

【0035】

【課題を解決するための手段】上記課題を解決するための一つの発明であるマルチメディアデータ送信装置は、複数のオブジェクトで構成されるマルチメディアデータを送信するマルチメディアデータ送信装置(方法)であって、知的財産権保護情報が付加されたマルチメディアデータをビットストリームとして入力する入力手段(工程)と、入力したビットストリームのマルチメディアデータを、知的財産権保護データと非知的財産権保護データとに分割する分割手段(工程)と、前記知的財産権保護データと前記非知的財産権保護データとのリンク情報を更新するリンク情報更新手段(工程)と、前記非知的財産権保護データの伝送を行う非セキュアセッション及び前記知的財産権保護データの伝送を行うセキュアセッションを管理するセッション管理手段(工程)とを備えることを特徴とする。

【0036】また、上記課題を解決するための一つの発明であるマルチメディアデータ伝送装置(方法)は、複数のオブジェクトで構成されるマルチメディアデータを送信するマルチメディアデータ送信装置(方法)であって、マルチメディアデータと、前記マルチメディアデータの知的財産権保護のための知的財産権保護データとを入力する入力手段(工程)と、前記マルチメディアデータの伝送を行う非セキュアセッション及び前記知的財産権保護データの伝送を行うセキュアセッションを管理するセッション管理手段(工程)とを備えることを特徴とする。

【0037】また、上記課題を解決するための一つの発明である記憶媒体は、上記送信方法の各工程に対応するプログラムコードを格納すること特徴とする。

【0038】また、上記課題を解決するための一つの発明であるマルチメディアデータ受信装置(方法)は、マルチメディアデータを受信するマルチメディアデータ受信装置(方法)であって、非セキュアセッションによりメディアデータを受信する第1の受信手段(工程)と、セキュアセッションにより前記メディアデータに対する知的財産を保護管理する知的財産保護管理データを受信

する第2の受信手段(工程)と、前記非セキュアセッション及び前記セキュアセッションを管理するセッション管理手段(工程)と、前記セッション管理手段(工程)により、前記非セキュアセッションを介して受信したメディアデータを、各メディアストリームに分割し、デコードする第1の処理手段(工程)と、前記セッション管理手段(工程)により、前記セキュアセッションを介して受信した知的財産保護管理データをデコードする第2の処理手段(工程)と、前記第1、第2の処理手段(工程)によりデコードされたデータに基づいて再生する再生手段(工程)とを備えることを特徴とする。

【0039】また、上記課題を解決するための一つの発明である記憶媒体は、上記受信方法の各工程に対応するプログラムコードを格納することを特徴とする。

【0040】また、上記課題を解決するための一つの発明であるマルチメディアデータ伝送システムは、複数のオブジェクトで構成されるマルチメディアデータの伝送システムであって、知的財産保護管理データが付加されたマルチメディアデータをビットストリームとして入力する入力手段と、入力したビットストリームのマルチメディアデータを、知的財産保護管理データとそれ以外のメディアデータとに分割する分割手段と、前記知的財産保護管理データと前記メディアデータとのリンク情報を更新するリンク情報更新手段と、前記メディアデータの伝送を行う非セキュアセッション及び前記知的財産保護管理データの伝送を行うセキュアセッションを管理するセッション管理手段と、前記非セキュアセッションを介して伝送されたメディアデータを、各メディアストリームに分割し、デコードする第1の処理手段と、前記セキュアセッションを介して受信した知的財産保護管理データをデコードする第2の処理手段と、前記第1、第2の処理手段によりデコードされたデータに基づいて再生する再生手段とを備えることを特徴とする。

【0041】また、上記課題を解決するための一つの発明であるマルチメディアデータ伝送システムは、複数のオブジェクトで構成されるマルチメディアデータの伝送システムであって、メディアデータと、前記メディアデータの知的財産の保護管理のための知的財産保護管理データとを入力する入力手段と、前記メディアデータの伝送を行う非セキュアセッション及び前記知的財産保護管理データの伝送を行うセキュアセッションを管理するセッション管理手段と、前記非セキュアセッションを介して伝送されたメディアデータを、各メディアストリームに分割し、デコードする第1の処理手段と、前記セキュアセッションを介して受信した知的財産保護管理データをデコードする第2の処理手段と、前記第1、第2の処理手段によりデコードされたデータに基づいて再生する再生手段とを備えることを特徴とする。

【0042】

【発明の実施の形態】以下、添付図面に従って本発明に

係る実施の形態を詳細に説明する。

【0043】図1は、第1の実施形態におけるシステム構成図である。

【0044】図中、101はオブジェクトディスクリプタ(OD)生成器であり、メディアエンコーダ105で処理対象となっているメディアデータの属性情報を符号化し、各種のODを生成する。102は、1PMPディスクリプタ生成器であり、メディアエンコーダ105で処理対象となっているメディアデータ、及びBIFSエンコーダ103で処理対象となっているシーン情報の著作権情報や再生条件等の知的財産保護情報を符号化して、当該符号化データを1PMPに関するディスクリプタ(1PMPディスクリプタ及び1PMP_ES)を生成する。103は、BIFSエンコーダであり、シーン情報を生成する。

【0045】105は、各種のメディアエンコーダであり、ビデオ・オーディオなどのメディアデータをエンコードする。104は、1PMP制御器であり、メディアエンコーダの出力するビットストリームを適宜降号化したり、また、暗号化に必要な鍵データを生成する。尚、1PMPの処理方法については、暗号化に限定するものではない。

【0046】106は、マルチプレクサであり、OD生成器101、1PMPディスクリプタ生成器102、BIFSエンコーダ103、1PMP制御器104、及びメディアエンコーダ105の各出力をマルチプレクスして、図4や図5に示すような1本のビットストリームへとまとめる部分である。同時に、各メディアの同期制御も行い、具体的には、タイスタンプやクロックリファレンスをバケットの中に埋めこむような作業を行う。これによって、パケット化されたビットストリームが完成したことになる。

【0047】以下、このビットストリームをネットワークを通じて伝送するときの方法を説明する。

【0048】107はセクタ(デマルチプレクサ)であり、マルチプレクサ106から出力されるビットストリームを、例えば1PMPディスクリプタや1PMP_ESなどのセキュリティに関するセキュリティビットストリーム(1PMPデータ)と、それ以外のビットストリーム(ビデオやオーディオ等のメディアビットストリーム)とに再分割する。120はセッションマネージャであり、送信側・受信側に対して最適なセッション(あるいはチャネル)をセットアップする。尚、セッションマネージャ120は図1上では1つしかないように図示されていますが送信側及び受信側にも夫々備わる。

【0049】このときのセッション(チャネル)セットアップ情報を格納しているのが123のセッション(チャネル)メッセージデータセットである。124は、セッション(チャネル)をセットアップするための、セキュリティ情報を格納しており、各セッション(チャネ

ル)がセキュアな接続を要求するかどうかを判定する。

【0050】121は、URLコンパートである。これは、セレクト107でビットストリームを再分割したために、メディアビットストリームとセキュリティビットストリームのリンク関係が異なってくることに対応するために処理が行われる。具体的には、1本のビットストリーム時には、メディアビットストリームとIPMPデータとが1D(具体的には、ビットストリーム内でユニークな整数値で示される)でリンクされているが、この2つのストリームが別体となるために、1Dの部分でURLストリングで置きかえる。URL自体の表記法については別途規格化されているがここでは詳細に記さないが、メディアビットストリームあるいは、IPMPデータの伝送チャンネルナンバーなどで示すことが可能である。

【0051】108はマルチプレクサであり、上記URLの交換情報に応じて、セキュリティに関するビットストリームに対して、必要があれば再度パケットサイズを行う。122はマルチプレクサであり、セレクト107で得られたマルチメディアビットストリームに対して、必要に応じて再度パケットサイズを行う。

【0052】このセキュリティビットストリームは、109のセキュアなセッションによって伝送される。

【0053】一方、通常のマルチメディア(A/V(Audio/Video))ビットストリームは110のセキュアでないセッションによって伝送される。しかしながら、すでに暗号化されているので、ネットワーク上で盗み見される恐れはない。111はデマルチプレクサであり、セキュアセッション109から伝送されてきたセキュリティビットストリームからIPMPディスクリプタおよびIPMP_ESを分離する。112はデマルチプレクサであり、セキュアでないセッション(ノンセキュアセッション)110から伝送されてきたマルチメディアビットストリームから、OD、BIFS、A/V(オーディオ/ビデオ)ビットストリームを分離する。

【0054】113はODパースであり、デマルチプレクサ112で得られたODのビットストリームからOD情報を抽出し、デコーダに必要な各情報をセットする。114はIPMPディスクリプタパースであり、デマルチプレクサ111によって得られたセキュリティビットストリームからIPMPディスクリプタ及びIPMP_ESをデコードする。115はBIFSデコーダであり、デマルチプレクサ112で得られたBIFSのビットストリームをデコードしてシーン情報を再構築する。116はIPMPコントローラであり、IPMPディスクリプタパース114によってデコードされたIPMPディスクリプタ及びIPMP_ES(知的財産管理情報)を元に、メディアデコーダ117または、レンダー119を制御(メディアの再生制限や効果制御等)する。具体的には、暗号が解読された場合にのみメディア

デコーダを駆動したり、デコードされた画像からの透かし情報を抽出し、再生制御に使うような方式が考えられる。117はメディアデコーダであり、デマルチプレクサ112で得られたA/Vのビットストリーム(イメージ・ビデオ・オーディオなどのメディアストリーム)をデコードする。118は同期制御部であり、各種メディア間の同期を司る。

【0055】図14に、本発明でのメッセージデータの一例を載せる。図13との違いは、ループの中にSecureデータ(1バイト)が挿入されていることである。この1バイトのデータによって、各チャンネルがセキュアであるかないかを識別する。

【0056】図12にこのAPIの一例を示す。1201は、アプリケーションから新規チャンネルを追加セットアップするインターフェースであり、1202は端末のネットワーク間におけるチャネルセットアップインターフェースとなっている。1203は、ネットワーク上において、実際の通信プロトコルなどをセットアップするAPIである。

【0057】従来例である図11との違いは、上述したように各チャンネルがセキュアであるかないかを識別するためデータであるSecureを有する。図16に、本発明での端末間のトランザクション図を示す。

【0058】従来例である図15との違いは、DA_ChannelAdd(), DN_TransMuxSetup(), DN_ChannelAdded()の各APIのパラメータとして、図14で示したSecureデータが追加されている点である。

【0059】以上のような構成における特徴は、セキュリティ情報を再抽出して、セキュアなセッション(もしくはチャンネル)にて伝送しているため、セキュリティ情報を盗み見される危険性がなくなる。

【0060】この様子を図10に示す。セキュリティ情報はセキュアなセッション(チャンネル)にて伝送され、盗み見ができないようになっていることがわかる。

【0061】従って、IPMPディスクリプタおよびIPMP_ESのシンタックスを定義してもセキュリティレベルを落とすことなく相互互換性を保つことが可能になる。

【0062】なお、説明が前後するが、図1の構成のほとんどは、ソフトウェアによって実現するものである。

また、図示ではセッションマネージャ120、セッションセットアップデータセット123、セキュリティ情報発生器124は、送信側及び受信側双方に設けることになる。

【0063】＜第2の実施形態＞第2の実施形態におけるシステム構成を図2に示し、以下に説明する。尚、図2中で図1と同様に機能する構成部には同一符号を付し、その詳細な説明は省略する。

【0064】本例では、2つのマルチプレクサ106a、106bによって、IPMPディスクリプタ生成器102で得られるIPMPディスクリプタ及びIPMP

ESと、OD生成器101、BIFSエンコーダ103、IPMP削御器104、及びメディアエンコーダ105で得られるデータ（メディアデータ）とを個別にマルチプレクスするように構成している。すなわち、当初からセキュリティデータをマルチプレクスすることなく、別のファイルとして保存しておく形式を取っている。

【0065】従って、図1のセクタ107、マルチプレクサ108、122及びURLコンパクタ121を設ける必要がなく、すなわち再度セキュアであるべきセキュリティビットストリームと通常のメディアビットストリームを再分割する必要がない。

【0066】尚、この場合も、各セッション（チャネル）ごと情報は、223のメッセージデータセットの中に格納されている。

【0067】なお、図1、図2の例どちらにおいても、セッション間で同期が取られ、セキュリティ情報が伝送されてから、レンドラ119で再生や表示が開始されるべきであるのは言うまでもない。

【0068】また、上記実施形態では、ネットワークを構成するハードウェア等が含まれるものの、各処理部は実際はソフトウェアで実現できるものである。即ち、本発明の目的は、上述した実施の形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（または、記録媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（または、CPUやMPU）が、記憶媒体に格納されたプログラムコードを読み出し、実行することによっても達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が、上述した実施の形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体が本発明を構成することになる。

【0069】また、コンピュータが読み出したプログラムコードを実行することにより、上述した実施の形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（OS）等が、実際の処理の一部または全部を行い、その処理によって、上述した実施の形態の機能が実現される場合も含まれることは言うまでもない。

【0070】さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPU等が、実際の処理の一部または全部を行い、その処理によって、上述した実施の形態の機能が実現される場合も含まれることは言うまでもない。

【0071】

【発明の効果】以上説明したように本発明によれば、セキュリティを要する情報の安全性を保ちつつ、マルチメディア伝送を行うことが可能になる。

【図面の簡単な説明】

【図1】実施形態におけるシステム構成図である。

【図2】第2の実施形態におけるシステム構成図である。

【図3】レンドリング結果の例を示す図である。

【図4】ビットストリームの構造の一例を示す図である。

【図5】ビットストリームの構造の一例を示す図である。

【図6】IPMPディスクリプタの構造を示す図である。

【図7】従来のエンコーダ部を示す図である。

【図8】従来のデコーダ部を示す図である。

【図9】従来のストリーム伝送の例を示す図である。

【図10】実施形態のストリーム伝送の例を示す図である。

【図11】従来のチャネルセットアップAPIの構造を示す図である。

【図12】実施形態におけるチャネルセットアップAPIの構造を示す図である。

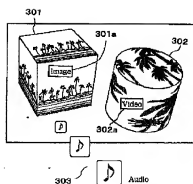
【図13】従来のチャネルセットアップメッセージの構造式を示す図である。

【図14】実施形態におけるチャネルセットアップメッセージの構造式を示す図である。

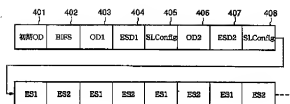
【図15】従来のチャネルセットアップトランザクションを示す図である。

【図16】実施形態におけるチャネルセットアップトランザクションを示す図である。

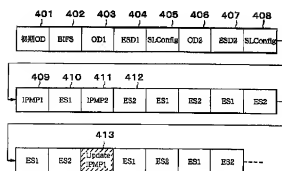
【図3】



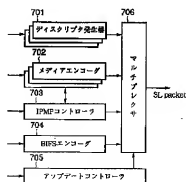
【図4】



【図5】



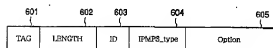
【図7】



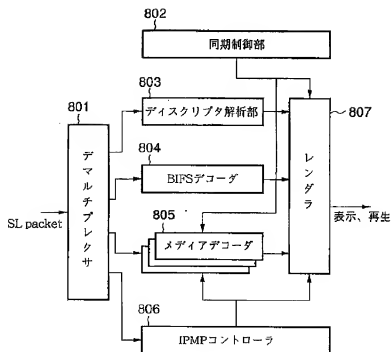
【図13】

| Syntax | Num. Of Bytes |
|---|----------------------------|
| <pre> EPL_ChannelAddrRequest() { domainMessageHeader() NetworkDomainId ServantId Count loopCount { CAT Direction qosDescriptor() ddiData() } } </pre> | 10 2 1 2 1 |

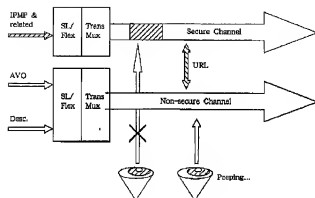
【図6】



【図8】



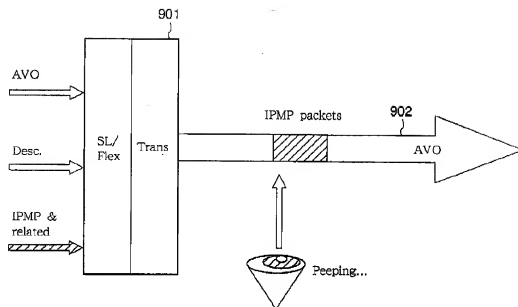
【図10】



【図14】

| Syntax | Num. Of Bytes |
|---------------------------|---------------|
| DS_ChannelAddressRequest{ | |
| descriptorHeader() | |
| NetworkSessionId | 10 |
| ServiceId | 2 |
| Count | 1 |
| loopcount{ | |
| CAT | |
| Direction | 2 |
| Secure | 1 |
| sessionIdDescriptor() | 1 |
| data() | |
| } | |

【図 9】



【図 12】

1201
 DA_ChannelAdd(IN:serviceSessionId,loop(qosDescriptor,
 direction,Secure,uuDataInBuffer,uuDataInLen);
 OUT:loop(response,channelHandle,uuDataOutBuffer,
 uuDataOutLen))

1202
 DN_ChannelAdd(IN:networkSessionId,serviceId,loop(CAT,
 direction,Secure,qosDescriptor,ddDataIn0);
 OUT:loop(response,TAT,ddDataOut0))

1203
 DN_TransMuxSetup(IN:networkSessionId,loop(TAT,
 direction,Secure,qosDescriptor,resource0);
 OUT:loop(response,resources0))

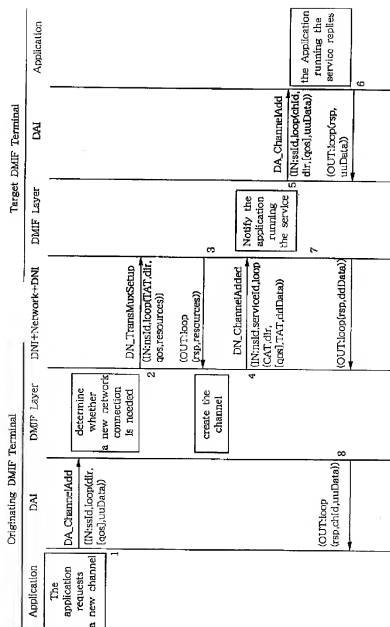
【図 11】

1101
DA_ChannelAdd(IN:serviceSessionId,loop(qosDescriptor,
direction,uuDataInBuffer,uuDataInLen);
OUT:loop(response,channelHandle,uuDataOutBuffer,
uuDataOutLen))

1102
DN_ChannelAdd(IN:networkSessionId,serviceId,loop(CAT,
direction,qosDescriptor,ddDataIn());
OUT:loop(response,TAT,ddDataOut()))

1103
DN_TransMuxSetup(IN:networkSessionId,loop(TAT,
direction,qosDescriptor;resource());
OUT:loop(response,resources()))

【図15】



【図 16】

